

(12) (9)文献

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-328460

(43)Date of publication of application : 30.11.1999

(51)Int.Cl.

G07B 15/00

(21)Application number : 10-125923

(71)Applicant : MITSUBISHI HEAVY IND LTD

(22)Date of filing : 08.05.1998

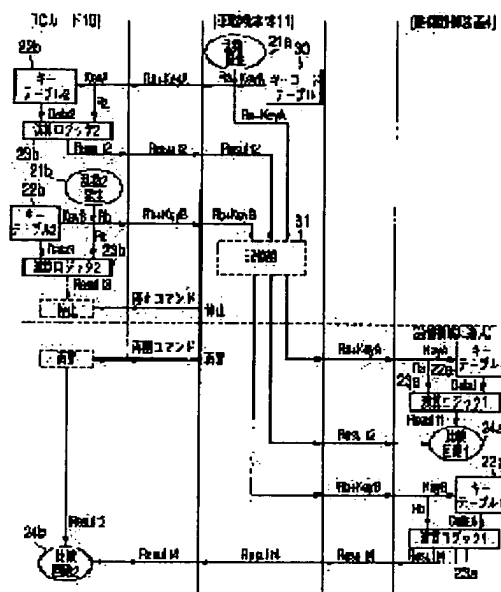
(72)Inventor : YASUI MASAYUKI

(54) METHOD FOR MUTUALLY CERTIFYING IC CARD FOR PAY ROAD

(57)Abstract:

PROBLEM TO BE SOLVED: To surely operate mutual certification of an IC card within a prescribed time in an inexpensive system, and to maintain security.

SOLUTION: When an IC card 10 is inserted, an on-vehicle equipment main body 11 transmits a random number 1 (Ra) and a key code (Key A) to the IC card 10 so that a certification operation can be executed. In the on-vehicle equipment main body 11, the random number 1 (Ra), key code (Key A), the arithmetic result 2 (result 2) of the IC card 10, random number 2 (Rb), and key code (Key B) are stored in a storage part 31, and a stop command is transmitted to the IC card 10. When the on-vehicles device enters a communication area in this state, the on-vehicle equipment main body 11 transmits the storage information in the storing part 31 to a road side controller 4 so that the certification operation can be executed, and transmits a resume commands and an arithmetic result 4 (Result 4) of the road side controller 4 to the IC card 10. The IC card 10 confirms the validity of the road side controller 4 according to the already obtained arithmetic result 3 (Result 3) and the arithmetic result 4 (Result 4).



LEGAL STATUS

[Date of request for examination] 17.04.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3697061

[Date of registration] 08.07.2005

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(11)特許出願公開番号

(43)公開日 平成11年(1999)11月30日

510

審査請求 未請求 請求項の数 2 OL (全 7 頁)

(71)出題人 000006208

東京都千代田区丸の内二丁目5番1号

(72) 発明者 泰井 真之

兵庫県神戸市兵庫区和田崎町一丁目1番1

号 三菱重工業株式会社神戸造船所内

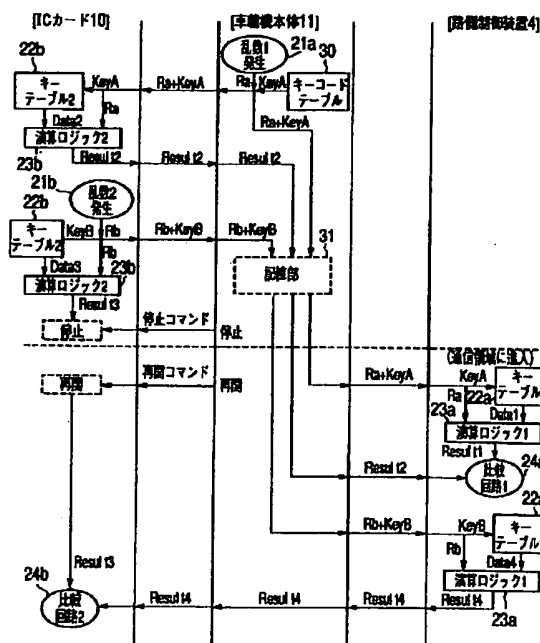
(74)代理人 弁理士 鈴江 武彦 (外5名)

(54) 【発明の名称】 有料道路のＩＣカード相互認証方法

(57) 【要約】

【課題】安価なシステムで所定の時間内でＩＣカードの相互認証を確実にしない、且つ、高いセキュリティを保持する。

【解決手段】車載機本体１１はＩＣカード１０が挿入されると、乱数１（Ra）とキーコード（Key A）をＩＣカード１０へ送信し認証演算を実行させる。車載機本体１１は、乱数１（Ra）、キーコード（Key A）、ＩＣカード１０の演算結果２（Result2）、乱数２（Rb）、キーコード（Key B）を記憶部３１に記憶し、ＩＣカード１０に停止コマンドを送信する。この状態で車載装置が通信領域に進入すると、車載機本体１１は記憶部３１の記憶情報を路側制御装置４へ送信し認証演算を実行させると共に、ＩＣカード１０に再開コマンド及び路側制御装置４の演算結果４（Result4）を送信する。ＩＣカード１０は、既に求めた演算結果３（Result3）と演算結果４（Result4）により路側制御装置４の正当性を確認する。



【特許請求の範囲】

【請求項1】 料金収受用のＩＣカード及び無線通信機能を備えた車載機本体からなる車載装置を車両に搭載し、有料道路の料金所に設置される路側制御装置との間で無線通信により情報を交換して料金収受を行なう際に、相手方の正当性を相互に認証する有料道路のＩＣカード相互認証方法において、

前記車載機本体に乱数発生部、キーコードテーブルを設けると共に、認証情報記憶用の記憶部を設け、前記車載機本体はＩＣカードが挿入されると、前記乱数発生部により乱数を発生させると共にキーコードテーブルよりキーコードを選択してＩＣカードへ送信して認証演算を実行させ、前記乱数、キーコード、及び前記ＩＣカードの演算結果を前記記憶部に記憶した後、前記ＩＣカードに停止コマンドを送信して該ＩＣカードの相互認証動作を一時停止させ、

前記車両に搭載された車載装置が料金所の通信領域に進入すると、車載機本体は前記記憶部の記憶情報を路側制御装置へ送信して認証演算を実行させると共に、前記ＩＣカードに再開コマンド及び前記路側制御装置の認証結果を送信して該路側制御装置に対する認証動作を実行させることを特徴とする有料道路のＩＣカード相互認証方法。

【請求項2】 前記記憶部は、認証完了後またはＩＣカードが車載機本体から引き抜かれた場合に記憶内容がクリアされるように構成したことを特徴とする請求項1記載の有料道路のＩＣカード相互認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、有料道路の通行料金自動徴収システムにおけるＩＣカードの相互認証方法に関する。

【0002】

【従来の技術】 図2は、本発明の対象とする有料道路の通行料金自動徴収システムの機器構成例を示すものである。図2において、1は車両、2は車両1に搭載される車載装置、3は料金所キャノピーなど路側に固定設置される路側アンテナ、4は車載装置2と路側アンテナ3間の通信制御及びデータ処理を行なう路側制御装置、5は路側アンテナ3と車載装置2との間で通信が可能な通信領域5を示す。

【0003】 車載装置2を搭載した車両1が料金所に近づき、通信領域5に進入すると、車載装置2と路側アンテナ3との間で無線通信が行なわれ、料金収受に必要な情報例えば経路情報、金額情報等が交換され、通行料金が自動的に徴収される。

【0004】 図3は、本発明の対象とする車載装置2の構成例を示すものである。車載装置2は、大別してＩＣカード10と車載機本体11に分けられる。ＩＣカード10は、マイクロプロセッサ及びメモリを内蔵したコン

タクト型カードで、金額情報、個人情報など高いセキュリティを必要とするデータが格納されている。

【0005】 車載機本体11は、ＩＣカード10とデータ転送するためのＩＣカードコンタクト部12及びＩＣカードインターフェイス回路13、上記路側アンテナ3と無線通信するためのアンテナ15及び無線制御部16、車両1内の運転者とインターフェイスとなる表示部17及び入力部18、これらＩＣカード10、無線通信、表示、入力及びデータを処理、記憶するマイクロプロセッサ14から構成される。

【0006】 そして、車載装置2を使用する時は、ＩＣカード10を車載機本体11に挿入した状態で有料道路を走行し、料金所の通信領域5に進入することで、ＩＣカード10内の残額情報、個人情報が車載機本体11を経由して路側アンテナ3及び路側制御装置4へ送信される。路側制御装置4で受信したＩＣカード10の残額情報、個人情報に基づきデータチェックを行ない、問題がなければ通行料金の引き去り後、新しい金額情報を路側アンテナ3、車載機本体11を経由してＩＣカード10へ書込む。

【0007】 上記のようにして通行車両1に対する料金収受処理が行なわれるが、ＩＣカード10内の金額情報、個人情報は、不正防止、秘匿性の観点より高いセキュリティが要求される。一般的に使用される不正防止方法としては、各々相手方の正当性を確認する相互認証方法が用いられている。

【0008】 図4は、一般的なＩＣカードの認証方法例を示したものである。ＩＣカード10及びＩＣカード端末機は、それぞれ乱数発生部21a、21b、キーコードに対応する認証用データを格納するキーテーブル22a、22b、認証用演算ロジック23a、23b、演算結果を比較する比較回路24a、24bを有する。

【0009】 まず、ＩＣカード端末機からＩＣカード10を認証する場合について説明する。ＩＣカード端末側の乱数発生部21aで乱数1(Ra)を発生させ、キーテーブル22aよりキーコード(Key A)を任意に選定する。ＩＣカード端末機は乱数1(Ra)とキーコード(Key A)に対応する認証用データ(Data1)より演算ロジック23aにて認証演算を行ない、演算結果1(Result1)を得る。

【0010】 一方、乱数1(Ra)とキーコード(Key A)はＩＣカード10へ送信され、ＩＣカード10は乱数1(Ra)とキーテーブル22bよりキーコード(Key A)に対応する認証用データ(Data2)を取出し、演算ロジック23bにて認証演算を行ない、演算結果2(Result2)を得る。ＩＣカード10の演算結果2(Result2)は、ＩＣカード端末機に送信され、ＩＣカード端末機の比較回路24aにてＩＣカード端末機の演算結果1(Result1)とＩＣカード10の演算結果2(Result2)が比較され、結果が一致していればＩＣカード10

の正当性を確認できる。

【0011】次に、ICカード10からICカード端末機を認証する場合について説明する。ICカード10からICカード端末機を認証する場合には、ICカード10側で乱数発生部21bから乱数2(Rb)を発生させ、キーテーブル22bよりキーコード(Key B)を任意に選定し、乱数2(Rb)と認証用データ(Data3)より演算ロジック23bにて認証演算を行ない、演算結果3(Result3)を得る。

【0012】上記乱数2(Rb)とキーコード(Key B)は、ICカード端末機に送信され、ICカード端末機は乱数2(Rb)とキーテーブル22aよりキーコード(Key B)に対応する認証用データ(Data4)を取出し、演算ロジック23aにて認証演算を行ない、演算結果4(Result4)を得る。この演算結果4(Result4)は、ICカードへ送信され、ICカード10の比較回路24bにてICカード演算結果3(Result3)とICカード端末機の演算結果4(Result4)が比較され、結果が一致していればICカード10はICカード端末機の正当性を確認できる。

【0013】

【発明が解決しようとする課題】図4の例では、ICカード10とICカード端末機が持つキーテーブル22a及び演算ロジック23aが解読されると不正使用される恐れがあり、このキーテーブル22a及び演算ロジック23aの高いセキュリティ性が必要となる。

【0014】一般的にICカード10のキーテーブル22b、演算ロジック23bは、ICチップ内に格納されており、高いセキュリティを有する。一方、ICカード端末機は、通常、銀行やデパート等の店舗に固定設置され、一般の利用者が安易に手を触れない場所にあり、店舗自体のセキュリティを上げることでICカード端末機のキーテーブル22a、演算ロジック23aのセキュリティが守られている。

【0015】しかし、有料道路の通行料金自動徴収システムの場合、図3に示した車載機本体11がICカード端末機となる。車載機本体11は、不特定多数の一般利用者に配られるため、悪意を持つ利用者が車載機本体11を分解し、車載機本体11内の認証用キーテーブル、演算ロジックを解析する可能性がある。

【0016】また、車載機本体11を単なる中継機とし、ICカード10と図2に示した路側制御装置4間で相互認証を行なう方法が考えられるが、車載装置2と路側アンテナ3間が通信可能な時間は通信領域5の大きさと車両走行速度に影響される。例えば通信領域5を3m、車両走行速度を時速54kmと仮定すると、車載装置2と路上アンテナ3間の通信時間は、「 $3\text{m} \div 54\text{km/h} = 0.2\text{秒}$ 」となり、この0.2秒以内に相互認証を完了させる必要がある。但し、通信領域5が小さい場合や車両走行速度が速くなると、通信可能な時間は更

に短くなり、相互認証演算時間もそれに伴って短くする必要がある。更に、演算ロジックについてもセキュリティ性を高めるため複雑な演算式が必要であり、複雑な演算式ほど演算時間がかかる。

【0017】一般的にICカードのマイクロプロセッサは動作速度が遅く、複雑な演算式を計算するのに数百msの時間が必要であり、走行中の車両に搭載されたICカードと路側制御装置間で相互認証することは時間的に困難である。

【0018】その対策として、ICカードの演算時間を早くするためマイクロプロセッサの動作速度を早くする方法や数値演算プロセッサを搭載する方法が考えられるが、これらの方法ではICカードが高価なものになるという問題があった。

【0019】本発明は上記の課題を解決するためになされたもので、車載機本体に高いセキュリティが必要なキーテーブルと演算ロジックを格納する必要がなく、ICカードに使用されるマイクロプロセッサの動作速度が遅くても料金収受処理を円滑に行なうことができる有料道路のICカード相互認証方法を提供することを目的とする。

【0020】

【課題を解決するための手段】第1の発明は、料金収受用のICカード及び無線通信機能を備えた車載機本体からなる車載装置を車両に搭載し、有料道路の料金所に設置される路側制御装置との間で無線通信により情報を交換して料金収受を行なう際に、相手方の正当性を相互に認証する有料道路のICカード相互認証方法において、前記車載機本体に乱数発生部、キーコードテーブルを設けると共に、認証情報記憶用の記憶部を設け、前記車載機本体はICカードが挿入されると、前記乱数発生部により乱数を発生させると共にキーコードテーブルよりキーコードを選択してICカードへ送信して認証演算を実行させ、前記乱数、キーコード、及び前記ICカードの演算結果を前記記憶部に記憶した後、前記ICカードに停止コマンドを送信して該ICカードの相互認証動作を一時停止させ、前記車両に搭載された車載装置が料金所の通信領域に進入すると、車載機本体は前記記憶部の記憶情報を路側制御装置へ送信して認証演算を実行させると共に、前記ICカードに再開コマンド及び前記路側制御装置の認証結果を送信して該路側制御装置に対する認証動作を実行させることを特徴とする。

【0021】第2の発明は、前記第1の発明において、認証完了後またはICカードが車載機本体から引き抜かれた場合に記憶部の記憶内容がクリアされるように構成したことを特徴とする。

【0022】

【発明の実施の形態】以下、図面を参照して本発明の一実施形態を説明する。図1は、本発明に係る有料道路のICカード相互認証方法を説明するための図である。本

実施形態は、図2に示した路側制御装置4に、キーコードに対応する認証用データを格納するキーテーブル22a、認証用演算ロジック23a、この演算ロジック23aによる演算結果1 (Result1) と車載機本体11の演算結果を比較する比較回路24aを備えている。

【0023】また、図3に示した車載機本体11には、乱数発生部21a、キーコードだけが格納されているキーコードテーブル30、及び認証用の各データを記憶する記憶部31を設けている。この記憶部31は、認証完了後、またはICカード10が車載機本体11から引き抜かれた場合に記憶内容がクリアされるようになっている。

【0024】そして、図3に示したICカード10には、乱数発生部21b、キーテーブル22b、演算ロジック23b、比較回路24bを設けている。次に本発明の実施形態に係る有料道路のICカード相互認証方法について説明する。

【0025】車両の走行に際し、ICカード10を車載機本体11に挿入すると、車載機本体11は乱数発生部21aより乱数1 (Ra) を発生させ、キーコードだけが格納されているキーコードテーブル30よりキーコード (Key A) を選択し、乱数1 (Ra) とキーコード (Key A) をICカード10へ送信する。

【0026】ICカード10は、乱数1 (Ra) とキーテーブル22bよりキーコード (KeyA) に対する認証用データ (Data2) を取出し、演算ロジック23bにて認証演算を行ない、演算結果2 (Result2) を得る。このICカード10の演算結果2 (Result2) は、車載機本体11へ送信される。

【0027】次にICカード10は、乱数発生部21bから乱数2 (Rb) を発生させ、キーテーブル22bよりキーコード (Key B) を任意に選定し、乱数2 (Rb) とキーテーブル22bから取り出した認証用データ (Data3) より演算ロジック23bにて認証演算を行ない、演算結果3 (Result3) を得る。上記乱数2 (Rb) とキーコード (Key B) は、車載機本体11へ送信される。

【0028】車載機本体11は、乱数発生部21aで発生した乱数1 (Ra)、キーコード (Key A)、ICカード10から送信されてきた演算結果2 (Result2)、乱数2 (Rb)、キーコード (Key B) を一旦記憶部31に記憶すると共に、ICカード10に対して相互認証の一時停止を指示する停止コマンドをICカード10へ送信する。停止コマンドを受信したICカード10は、相互認証を一時停止する。

【0029】この状態で図2に示すように車載装置2を搭載した車両1が通信領域5に進入し、車載装置2と路側アンテナ3の通信が可能となった場合、車載機本体11は、まず記憶部31に記憶していた車載機本体11で発生した乱数1 (Ra) とキーコード (Key A) を路側制御装置4へ送信し、続いてICカード10での演算結果

2 (Result2) を路側制御装置4へ送信する。

【0030】路側制御装置4は、乱数1 (Ra) とキーテーブル22aよりキーコード (KeyA) に対応する認証用データ (Data1) を取出し、演算ロジック23aにて認証演算を行ない、演算結果1 (Result1) を得る。この演算結果1 (Result1) と車載機本体11の記憶部31から送られてきたICカード10の演算結果2 (Result2) とを比較回路24aで比較し、結果が一致していれば路側制御装置4はICカード10の正当性を確認できる。

【0031】次に車載機本体11は、記憶部31に記憶している情報、すなわち、ICカード10より受信した乱数2 (Rb) とキーコード (Key B) を路側制御装置4へ送信する。

【0032】路側制御装置4は、乱数2 (Rb) とキーテーブル22aよりキーコード (KeyB) に対応する認証用データ (Data4) を取出し、演算ロジック23aにて認証演算を行ない、演算結果4 (Result4) を得る。この演算結果4 (Result4) は、車載機本体11に送信される。

【0033】車載機本体11は、通信領域5に進入することで、ICカード10に対して相互認証停止を解除するための再開コマンドを送信する。また、車載機本体11は、路側制御装置4から受信した演算結果4 (Result4) をICカード10へ送信する。

【0034】ICカード10は、上記車載機本体11からの再開コマンドにより動作を再開し、既に演算ロジック23bで求めた演算結果3 (Result3) と路側制御装置4の演算結果4 (Result4) を比較回路24bで比較し、路側制御装置4の正当性を確認する。この場合、ICカード10は、上記比較回路24bでの比較結果が一致していれば、路側制御装置4の正当性を確認できる。

【0035】車載機本体11の記憶部31は、上記認証完了後、またはICカード10が車載機本体11から引き抜かれた場合に記憶内容がクリアされる。上記のように認証完了後、またはICカード10が車載機本体11から引き抜かれた場合に記憶部31の記憶内容をクリアすることにより、車載機本体11を分解したとしても記憶部31の記憶内容を盗み出すことは困難である。もし、記憶部31の内容を読み出すことができたとしても、記憶部31には乱数、キーコード、演算結果しか格納されていないので、それから認証用データ、認証ロジックを導き出すことは難しく、非常に高いセキュリティを持たせることができる。

【0036】

【発明の効果】以上詳記したように本発明によれば、車載機本体にICカードの認証演算を事前に実施するための必要最小限な乱数発生部、キーコードテーブルを設けると共に、乱数、キーコード、演算結果を記憶する記憶部を搭載し、ICカード側の認証演算を料金所の通信領

域進入前に実施するようにしたので、車載機本体に高いセキュリティが必要なキーテーブルと演算ロジックを格納する必要がなく、安価に構成することができる。また、上記のようにICカード側の認証演算を料金所の通信領域進入前に実施することにより、ICカードに使用されるマイクロプロセッサの動作速度が遅くても、全くその影響を受けない。更に、車載機本体に設けた記憶部は、認証完了後、またはICカードが引き抜かれた場合にクリアされるようにしているので、車載機本体を分解して記憶部の内容を盗み出すことは困難であり、もし、記憶部の内容を読み出すことができたとしても、記憶部には乱数、キーコード、演算結果しか格納されていないので、それらの情報から認証用データ、認証ロジックを導き出すことは難しく、非常に高いセキュリティを持たせることができる。従って、本発明による有料道路のICカード相互認証方法を採用することにより、安価で不正防止に優れた有料道路の通行料金自動徴収システムを構築することができる。

【図面の簡単な説明】

【図1】本発明の一実施形態に係る有料道路のICカード相互認証方法を示す図。

【図2】本発明の対象とする有料道路の通行料金自動徴収システムの機器構成例を示す図。

【図3】図2における車載装置の構成例を示すブロック*

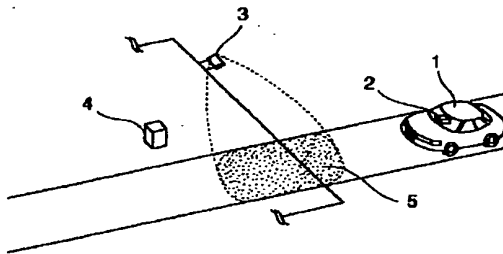
*図。

【図4】従来の有料道路のICカード相互認証方法を示す図。

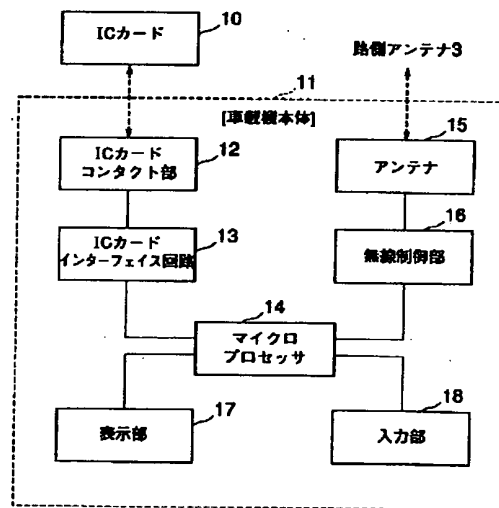
【符号の説明】

- 1 車両
- 2 車載装置
- 3 路側アンテナ
- 4 路側制御装置
- 5 通信領域
- 10 車載機本体
- 11 ICカードコンタクト部
- 12 ICカードインターフェイス回路
- 13 マイクロプロセッサ
- 14 アンテナ
- 15 無線制御部
- 16 表示部
- 17 入力部
- 21a、21b 乱数発生部
- 22a、22b キーテーブル
- 23a、23b 演算ロジック
- 24a、24b 比較回路
- 30 キーコードテーブル
- 31 記憶部

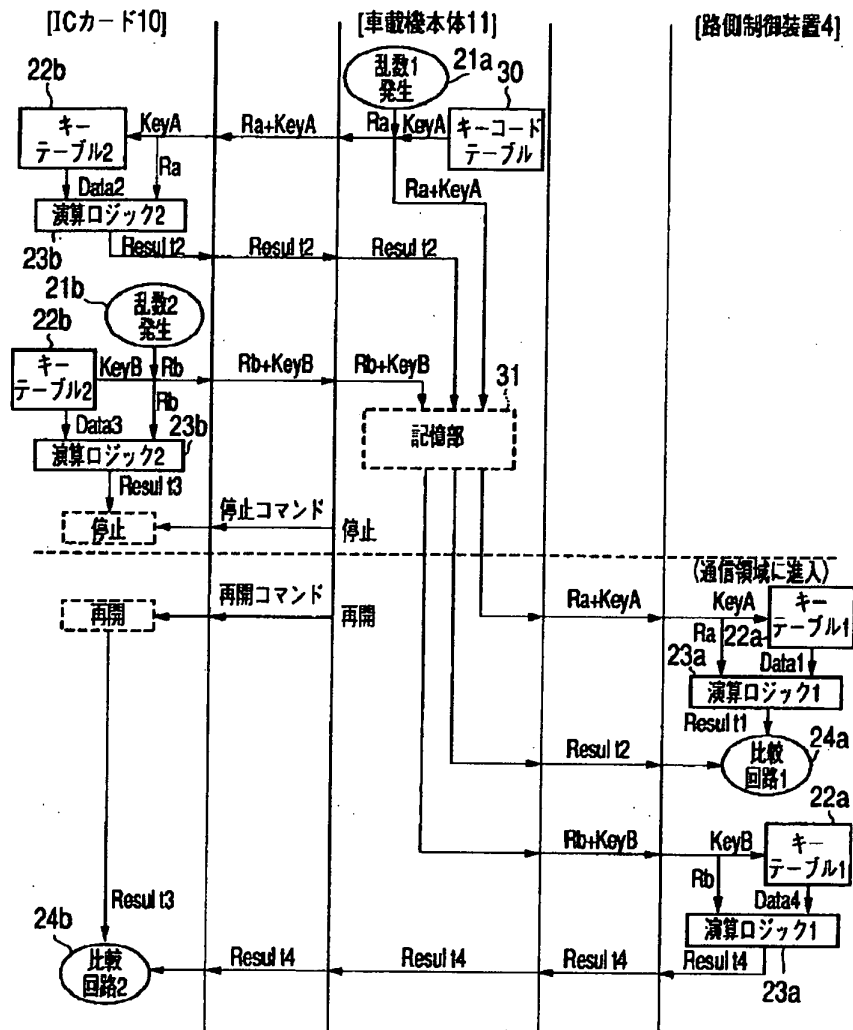
【図2】



【図3】



〔図1〕



【図4】

